PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 :
G06F 1/00

A2

(11) International Publication Number: WO 00/70428

(43) International Publication Date: 23 November 2000 (23.11.00)

(21) International Application Number: PCT/US00/12701

(22) International Filing Date: 9 May 2000 (09.05.00)

(30) Priority Data:
09/312,293 14 May 1999 (14.05.99) US

(71) Applicant: THE PROCTER & GAMBLE COMPANY [US/US]; One Procter & Gamble Plaza, Cincinnati, OH 45202 (US).

(72) Inventors: BERGER, Andrea, Turco; 7823 Shadowhill Way, Cincinnati, OH 45224 (US). TELLJOHANN, Michael, Alan; 8728 Tanagerwoods Drive, Cincinnati, OH 45249 (US). KUNS, Richard, Michael; 5714 Sigmon Way, Fairfield, OH 45014 (US). McFADDEN, Terrence, Paul; 1252 Meriweather Avenue, Cincinnati, OH 45208 (US). LEE, Samuel, Augustine; 2308 Morelein, Cincinnati, OH 45219 (US). HOOG, Jason, Alan; 20642 Heather Ct., Lawrenceburg, IN 47025 (US).

(74) Agents: REED, T., David et al.; The Procter & Gamble Company, 5299 Spring Grove Avenue, Cincinnati, OH 45217-1087 (US).

(81) Designated States: AE, AL, AM, AT, AT (Utility model), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), DM, EE, EE (Utility model), ES, FI, FI (Utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: METHOD AND APPARATUS FOR SECURING AUTOMATIC ENTRY OF PASSWORD INFORMATION ASSOCIATED WITH A WEB SITE

(57) Abstract

The apparatus and method of the present invention provides increased security and efficiency in entering passwords for various web sites on an intranet or the Internet. The first time a message requesting a password is received from an intranet web site, the user name and password are recorded in volatile memory. On subsequent password requests from the same or any other intranet web site, the recorded user name and password are transmitted to the requesting web site without prompting the user. When the network session ends, the recorded data is erased or lost. Similarly, the first time a message requesting a password is received from an Internet web site, the user name and password are recorded on a secure server. On subsequent password requests from the same web site, the recorded user name and password may be retrieved from the secure server and transmitted to the requesting web site without prompting the user.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

METHOD AND APPARATUS FOR SECURING AUTOMATIC ENTRY OF PASSWORD INFORMATION ASSOCIATED WITH A WEB SITE

FIELD OF THE INVENTION

The present invention relates in general to a method and apparatus for automatically entering network password information and in particular to automatically entering network password information in response to a password request from an intranet or Internet web site while maintaining a secure environment.

BACKGROUND OF THE INVENTION

Networked environments, such as an intranet or the Internet, allow people using local network devices to request information from remote network devices. Typically, the local network device (i.e., the user device) is a personal computer (PC) executing client software (e.g., a web browser), and the remote network device is typically a web site. Data may be retrieved from a web site by sending a request to a unique address associated with the web site. Typically, the unique address is a Uniform Resource Locator (URL).

Upon request, each web site transmits data related to one or more web pages such as text, graphics, and hypertext markup language (HTML) files to the user device over the network. Certain web sites require the user to be authorized in order to access some or all of the associated web pages. Typically, the user identifies himself as an authorized user by responding to a password prompt displayed on the user device, wherein the password prompt provides blank fields for a user name and a password.

In some instances. after a predetermined period of inactivity (e.g., 15 minutes), the user must re-enter his user name and password in order to access data on that server. Further. many servers require their own authorization step even if they are working together in what appears to the user to be one seamless environment. As a result, the user must remember and enter his password fairly often. Users are often frustrated by the repetition.

As a result, prior art systems often include an option whereby user names, passwords, and the associated URL may be encrypted and stored on the user's hard drive in a password file. Subsequently, when a password prompt is detected from a known URL, the user name and password may be automatically entered into the blank fields.

These prior art approaches suffer from significant drawbacks. First, in an intranet environment, the user may be requesting data from a plurality of different servers (e.g., one hundred) without realizing she is doing so. The collection of servers may operate behind the scenes to present one seamless environment to the user, even though each server may require separate authentication. Because each server is associated with a unique URL, there are as many entries in the encrypted password file as there are servers. Many password systems require the user to change his password periodically for security reasons. As a result, prior art systems prompt the user once for each server (e.g., one hundred prompts). Changing what appears to the user to be one password (i.e., his intranet password) requires a plurality of entries. This process wastes time and frustrates the user.

Further, the password file is susceptible to attack. If several users share a PC or a user leaves his PC unattended for a short time, a hacker may copy the password file and proceed to decrypt the file on another machine. Once the password file is decrypted, the authorized data is compromised.

SUMMARY OF THE INVENTION

The present invention is directed to a computing device and program for automatically entering password information associated with a web site. The method and apparatus provides increased security and efficiency in entering passwords for various web sites on an intranet or the Internet.

In one aspect. the invention is directed to a method and apparatus for entering a password associated with a first web site and a second web site on an intranet. The system detects a password request from the first web site. Subsequently, the system writes password data exclusively in a volatile memory without having the password data being stored in a non-volatile memory. The password data is entered by a user in response to the first password request. When the system detects a second password request from the second web site, the system reads the volatile memory to retrieve the password data. and transmits the password data to the second web site in response to the second password request.

These and other features and advantages of the present invention will be apparent to those of ordinary skill in the art in view of the detailed description of the preferred embodiment which is made with reference to the drawings, a brief description of which is provided below.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram of a computer network capable of utilizing the present invention;

FIG. 2 is a more detailed block diagram of the user device of FIG. 1; FIG. 3 is a flow chart of a program that can be implemented by the user device of FIG. 2 to enter passwords associated with an intranet in accordance with the teachings of the present invention; and

FIG. 4 is a flow chart of a program that can be implemented by the user device of FIG. 2 to enter passwords associated with Internet web sites in accordance with the teachings of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

A block diagram of a computer network 10 (including a plurality of connected devices) in which the present invention is utilized is illustrated in FIG. 1. Preferably, the network 10 includes an intranet 10a. Optionally, the network 10 also includes the Internet 10b. In such an instance, the intranet 10a and the Internet 10b may be connected by a proxy server 11, as is well known. The Internet 10b is a nationwide network of computers that includes, but is not limited to, the World Wide Web. An intranet 10a is a local or wide area network (typically internal to a specific entity such as a corporation) which may use Internet protocols.

The intranet 10a may include a secure server 12, a plurality of user devices 14, and a plurality of internal web sites 16a, each of which is coupled to the intranet 10a in a known manner. Similarly, a plurality of external web sites 16b may be coupled to the Internet 10b in a known manner. Often. each web site 16 has its own server. However, persons of ordinary skill in the art will readily appreciate that more than one web site may reside on the same server. In the preferred embodiment web site servers comprise secure servers. Accordingly, one or more of the internal web sites 16a may reside on the secure server 12.

Each web site 16 transmits data related to one or more web pages 18 to a user device 14 over the network 10. Certain web sites 16 require the user to identify himself as an authorized user by responding to a password prompt displayed on the user device 14. Often, a particular user's user name and password is the same for all internal web sites 16a (i.e., web sites 16a on the intranet 10a). Many web sites 16a require the user to periodically change her password for security reasons. Accordingly, a synchronization utility may be periodically executed by a server (e.g., the secure server 12) on the intranet 10a to update the password on all other internal web sites 16a.

During operation. the proxy server 11 acts as a firewall between the intranet 10a and the Internet 10b. When a user requests a web page 18 from an internal web site 16a, the browser transmits the request directly to the web site 16a as is conventional. However, when a user requests a web page 18 from an external web site 16b, the browser transmits the request to the proxy server 11. In turn, the proxy server 11 transmits the request to the web site 16b. When the requested information is returned, it also passes through the proxy server 11.

Typically, browsers are configured with information indicating what type of URLs are associated with internal web sites 16a. and all other URLs are assumed to be associated with external web sites 16b. For example, all internal web sites 16a for company "Xyz" might begin with "internal.xyz.com". This information is typically entered by the user or system administrator once and then stored in a local registry for subsequent retrieval (i.e., configurable in the browser). When a request for a web page is made, the browser may distinguish internal web sites 16a from external web sites 16b by examining the associated URL and comparing it to the predefined address strings.

A more detailed diagram of one of the user devices 14, is illustrated in FIG. 2. A controller 30 in the user device 14 preferably includes a volatile memory device, such as a random-access memory (RAM) 32, a program memory 34, which may be in the form of a read-only memory (ROM), and a microprocessor 36, all of which may be interconnected by an address/data bus 38. Preferably, the program memory 34 electronically stores a computer program that implements all or part of the method described below, and the program is preferably executed by the microprocessor 36. Typically, program memory 34 comprises RAM loaded from a hard disk. Some of the steps described in the method below may be performed manually or without the use of the user device 14.

As is well known, a volatile memory is one that loses its data when power to the memory is terminated. An example of a volatile memory is a RAM. A non-volatile memory is one that does not lose the data when power to the memory is terminated. Examples of non-volatile memory include ROM, hard disks, diskettes, etc.

A transmitter and receiver in the form of a conventional input/output (I/O) circuit 40, such as a modem or local area network card, for example, typically couples the controller 30 to the network 10. An input device 42, such as a keyboard, may be connected to the I/O circuit 40 via a line 44 for entering data and commands into the controller 30. Further, a visual display 46, such as a cathode ray tube (CRT) or liquid crystal display (LCD), may be connected to the I/O circuit 40 to receive data via a line 48 to generate visual displays of data generated during operation of the user device 14. The visual displays may include prompts for a user's name and/or password. The user device 14 may also be connected to the network 10 via a line 50 connected to the I/O circuit 40 to send and receive data to and from the web sites 16 or proxy server 11.

A flow chart of a computer program 60 that can be implemented by the user device 14 to enter passwords associated with an intranet in accordance with the teachings of the present invention is illustrated in FIG. 3. Preferably, the programmed steps are performed by the controller 30. Once the program 60 is initiated by the browser, the controller 30 may receive messages from other devices connected to the network 10 via the I/O circuit 40.

Preferably, the first time a message requesting a user name and/or password is received from an internal web site 16a, the programmed controller 30 prompts the user for the necessary data. Subsequently, the user name and password are recorded in volatile memory (e.g., in RAM 32, not on a hard disk), and the user name/password data is transmitted to the requesting web site 16a. On subsequent user name/password requests from the same or any other intranet web site 16a (with a synchronized password and user name), the controller 30 may transmit the recorded user name and/or password data without prompting the user. When the network session ends, the recorded user name/password data is erased or lost.

The program 60 begins at step 62 by looking for a password and/or user name request message. Preferably, the controller 30 determines that a password and/or user name request message has been received by periodically polling (e.g., every 20 milliseconds) for a password request dialog box. For example, in a Microsoft Windows® environment, the controller 30 could call an operating system routine that returns a list of the names of all open windows. Then, by searching the list for a specific name or names used by a particular web browser (e.g., "Enter user name and password"), the controller 30 could determine if a password request dialog box has appeared since the last time it checked.

Persons of ordinary skill in the art will appreciate that many other methods of detecting a password request are well known. For example, the controller 30 could make a low level system call to determine if a particular type of socket, indicative of a password request, has been opened. Further, interrupt driven methods may be employed. For example, the controller 30 may trap on the operating system window call that was going to create the password request dialog box.

Regardless of the method used, if a password and/or username has been received as determined at step 62 (e.g., a request dialog box is displayed or would have been displayed), the program 60 then determines at step 64 if the request originated from an internal web site 16a. Preferably, internal web sites 16a are identified by a unique string contained in the associated address. Typically, a web site 16 address is a Uniform Resource Locator (URL) that contains a string of characters uniquely identifying each web page 18 associated with that web site 16. Typically, organization-specific definitions may be retrieved from a registry commonly used to direct the browser when to not use the proxy server 11 as described in detail above.

If the request originated with an internal web site 16a, at step 66 the program 60 then determines if a password and/or user name associated with an internal web site 16a has already been entered and is stored in RAM 32 (or some other volatile memory). If the intranet user name and password are not in memory, the program 60 preferably acquires them via a password prompt (e.g., a dialog box in Microsoft Windows ®). In a preferred embodiment, the program 60 intercepts or hides a password dialog box displayed by the browser at step 68 and supplies a similar password dialog box at step 70. In other words, the controller 30 causes a prompt to be shown on the display 46. In response, the user enters her user name and/or password via the keyboard 42 (or other input device) at step 72. By supplying its own password prompt at step 70, the program's task of receiving the user's name and password at step 72 is simplified. However, persons of ordinary skill in the art will readily appreciate that the browser's dialog box could be used and the data would then be recovered using other known methods.

Once the user name and password data associated with this user are received, at step 74 the program 60 writes the data to RAM 32 (or some other volatile memory) in a known manner. Subsequently, at step 76 the user name and/or password may be read from RAM 32 and at step 78 transmitted to the requesting web site 16a. Persons of ordinary skill in the art will readily appreciate that if the username and/or password are already available to the controller 30, it need not read the data from RAM 32. For example, if the controller 30 has a local cache which still contains the data (because it just wrote the data to RAM 32), then step 76 may be omitted.

Subsequently, at step 62 the program 60 looks for another password and/or user name request message. If a request is detected at step 62, but the program 60 determines that it did not originate at an internal web site 16a (step 64 described in detail above), then the program 60 ignores the request and returns to step 62. However, if a password and/or user name request is detected from an internal web site 16a, and step 66 determines that the user name and password are already stored in RAM 32, then at step 76 the user name and/or password may be read from RAM 32, and at step 78 the user name and/or password may be transmitted to the requesting web site 16a without prompting the user for the user name or password data. Preferably, the password and/or user name is transmitted to the requesting web site via a browser application.

Subsequently, at step 80 the program 60 determines if the user name and password transmitted were valid for the requesting web site 16a. Typically, this determination is made by evaluating a message from the web site 16a indicating success or failure of the log on attempt. If the user name and password are valid for this web site 16a, at step 82 the program 60 preferably loads the web site data and returns to step 62. However, if the user name or password are incorrect, at step 84 the program 60 may display several options for the user to select from. Preferably, a dialog box is displayed with three options. Specifically, the options include "Retry". "Help", and "Cancel". At step 86, if the user selects the "retry" option, program 60 flow loops back to step 68 to allow the user to reenter her user name and/or password.

Alternatively, at step 88, if the user selects the "help" option, the program 60 preferably displays a text box at step 89 which contains information that may assist the user in correcting a problem associated with her user name and/or password. Preferably, the help text includes explanations for at least three scenarios. First, the user may not be authorized for the current web site 16a. Second, the user may have mistyped her user name and/or password. Third, the username and/or password may be out of synchronization with the rest of the internal web sites 16a due to an incompatibility with the synchronization software. If the user selects "cancel", or when the user has finished reading the help screen(s), control preferably returns to step 62.

If no password and/or user name request message is detected at step 62, at step 61 the program 60 checks if the host program has been terminated (e.g., check if any windows from web browser are still open). If the host program is still running, the program 60 loops between step 61 and step 62 until a request is received or the host program is terminated. If the host program is terminated, at step 82 the program 60 erases the user name and/or password data stored in RAM 32, thereby maintaining a secure environment. Subsequently, the program 60 exits. Persons of ordinary skill in the art will readily appreciate that deallocating RAM will also serve to effectively erase it. In other words, the data may still be in RAM. but there is no convenient way to locate it. Similarly, if the program 60 is inadvertently aborted (e.g., the computer crashes), the user name and/or password data stored in RAM 32 will typically be lost, thereby maintaining the secure environment.

The present invention may also be used to handle passwords associated with external web sites 16b (i.e., web sites on the Internet). A flow chart of a computer program 90 that can be implemented by the user device 14 to enter passwords associated with the Internet 10b in accordance with the teachings of the present invention is illustrated in FIG. 4. Preferably, the programmed steps are performed by the controller 30. Once the program 90 is initiated the controller 30 may receive messages from other devices connected to the network 10 via the I/O circuit 40.

Preferably, the first time a message requesting a user name and/or password is received from an external web site 16b, the controller 30 prompts the user for the necessary data, records that data by transmitting it to the secure server 12 in an encrypted format, and also transmits the user name/password data to the requesting web site 16b. On subsequent password requests from the same web site 16b, the controller 60 may retrieve the data from the secure server 12, decrypt the data, and transmit it to the requesting web site 16b without prompting the user.

The program 90 begins at step 114 by authenticating with the secure server 12. For example, a local user name and password may be required to ensure this user is authorized to use the secure server 12. The program 90 then proceeds at step 92 by looking for a password and/or user name request message. Preferably, the controller 30 determines that a password and/or user name request message has been received by periodically polling for a password request dialog box as described in detail above. If a password request dialog box is displayed (or would have been displayed), the program 90 then determines if the request originated with an external web site 16b at step 94. Preferably, internal web sites 16a are identified by a unique string contained in the associated address as described in detail above. External web sites 16b are all other (non-internal) web sites 16b.

If the request originated with an external web site 16b, at step 96 the program 90 then determines if a password and/or user name has already been stored on the secure server 12 for this particular web site 16b by checking for the associated address (e.g., URL) in the database 20 on the secure server 12. If there is no associated user name and/or password stored on the secure server 12, the program 90 preferably acquires them via a password prompt (e.g., a dialog box in Microsoft Windows®). The program 90 may intercept or hide a password dialog box displayed by the browser at step 98 and supplies a similar password dialog box at step 100 as described in detail above.

Once the user name and password data associated with this user for this web site 16b are received at step 102, the program 90 transmits the data (e.g., user name, password, and URL) to the secure server 12 at step 104 in a known manner. Subsequently, at step 106 the user name and/or password may be requested and subsequently received from the secure server 12 and at step 108 transmitted to the requesting web site 16b. Persons of ordinary skill in the art will readily appreciate that if the username and/or password are already available to the controller 30, it need not request them from the secure server 12. For example, if the controller 30 has a local copy in RAM 32, then step 106 may be omitted. In one embodiment, the secure server 12 sends a copy of some or all of the database 20 to the user device 14 with or without a request from the user device 14 for the data and with or without a password request from a web site 16b. In this manner, the user device 14 may have a local copy of the data in RAM 32.

Subsequently, at step 92 the program 90 looks for another password and/or user name request message. If a request is detected at step 92, but the program 90 determines that it did not originate at an external web site 16b (step 94 described in detail above), then the program 90 preferably passes the request to program 60 (i.e., intranet password processing) and returns to step 92. However, if a password and/or user name request is detected from an external web site 16b, and step 96 determines that a user name and password are already stored on the secure server 12 for this web site address (or there is a local copy in RAM 32), then at step 106 the user name and/or password may be requested and received (if not already in RAM 32), and at step 108 the user name and/or password may be transmitted to the requesting web site 16b without prompting the user for the data.

At step 91 the program 90 may check to see if the host program has terminated. If the host program has not terminated (e.g., at least one browser window remains), then the program loops between step 91 and step 92 until a request is received or the host program is terminated.

Subsequently, at step 110 the program 90 determines if the user name and password transmitted were valid for the requesting web site 16b. As described above, this determination is typically made by evaluating a message from the web site 16b indicating success or failure of the log on attempt. If the user name and password are valid for this web site 16b, at step 112 the program 90 preferably loads the web site data and returns to step 92. However, if the user name or password are incorrect, at step 114 the program 90 may display several options for the user to select from. Preferably, a dialog box is displayed with three options. Specifically, the options include "Retry", "Help", and "Cancel". At step 116, if the user selects the "retry" option, program 90 flow loops back to step 98 to allow the user to reenter her user name and/or password.

Alternatively, at step 118, if the user selects the "help" option, the program 90 preferably displays a text box at step 120 which contains information that may assist the user in correcting a problem associated with her user name and/or password (as described in detail above). If the user selects "cancel", or when the user has finished reading the help screen(s), control preferably returns to step 92.

If the host program is terminated at step 91, then the controller 30 may disconnect from the secure server 12 at step 112. Subsequently, the program 90 exits. Once disconnected, the user must re-authenticate to communicate with the secure server 12.

In summary, persons of ordinary skill in the art will readily appreciate that a method and apparatus for securing automatic entry of password information associated with a web site has been provided. Systems implementing the teachings of the present invention can enjoy increased security and efficiency in entering passwords for various web sites on an intranet or the Internet.

The foregoing description has been presented for the purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form disclosed. Many modifications and variations are possible in light of the above teachings. It is intended that the scope of the invention be limited not by this detailed description, but rather by the claims appended hereto.

What is claimed is:

1. A method for entering a password associated with a first web site and a second web site on an intranet, characterized in the steps of:

   detecting a first password request from the first web site;

   writing password data exclusively in a volatile memory without having the password data being stored in a non-volatile memory, the password data being entered by a user in response to the first password request, the password data representing a password;

   detecting a second password request from the second web site;

   reading the volatile memory to retrieve the password data; and

   transmitting the password data to the second web site in response to the second password request.

2. A method as defined in Claim 1 further comprising the step of determining if the second web site is an internal web site.

3. A method as defined in any of the preceding claims further comprising the step of erasing the password data from the volatile memory.

4. A method as defined in Claim 3 further comprising the step of determining that a host program has terminated, wherein the step of erasing the password data is performed in response to the determination that the host program has terminated.

5. A method as defined in any of the preceding claims further comprising the step of hiding a first password prompt and displaying a second password prompt.

6. An apparatus for entering a password associated with a first web site and a second web site on an intranet characterized in that:

   a receiver receives a first password request from the first web site and a second password request from the second web site;

a controller is operatively coupled to the receiver, the controller detecting the first password request and the second password request;

a display device is operatively coupled to the controller;

a user input device is operatively coupled to the controller for receiving password data, wherein the password data is entered by a user in response to a first password prompt;

a volatile memory device is operatively coupled to the controller; and

a transmitter is operatively coupled to the controller;

the controller causing the display device to display the first password prompt in response to the first password request, the controller causing the volatile memory device to write the password data exclusively in the volatile memory in response to the user input device receiving the password data without having the password data being stored in a non-volatile memory, the controller causing the volatile memory device to read the password data in response to the receiver receiving the second password request, and the controller causing the transmitter to send the password data in response to the detection of the second password request.

7. An apparatus as defined in Claim 6 wherein the controller is adapted to cause the volatile memory device to erase the password data from the volatile memory.

8. An apparatus as defined in Claim 6 or 7 wherein the controller is adapted to hide a second password prompt.

9. An apparatus for entering a password associated with a web site on the Internet characterized in that:

a receiver receives a first password request from the web site, a second password request from the web site, an address associated with the web site from the web site, the address associated with the web site from a secure server, and a password from the secure server;

a controller is operatively coupled to the receiver, the controller detecting the first password request, the second password request, the address from the web site, the address from the secure server, and the password;

a display device is operatively coupled to the controller;

a user input device is operatively coupled to the controller for receiving password data, wherein the password data is entered by a user in response to the first password prompt; and

a transmitter is operatively coupled to the controller;

the controller causing the display device to display a first password prompt in response to the first password request, the controller causing the transmitter to send the password data to the secure server in response to the user input device receiving the password data, and the controller causing the transmitter to send the password data to the web site in response to the detection of the second password request if the second password request originated from the address.

10. An apparatus as defined in Claim 9 wherein the controller is adapted to intercepting a command to display a second password prompt.

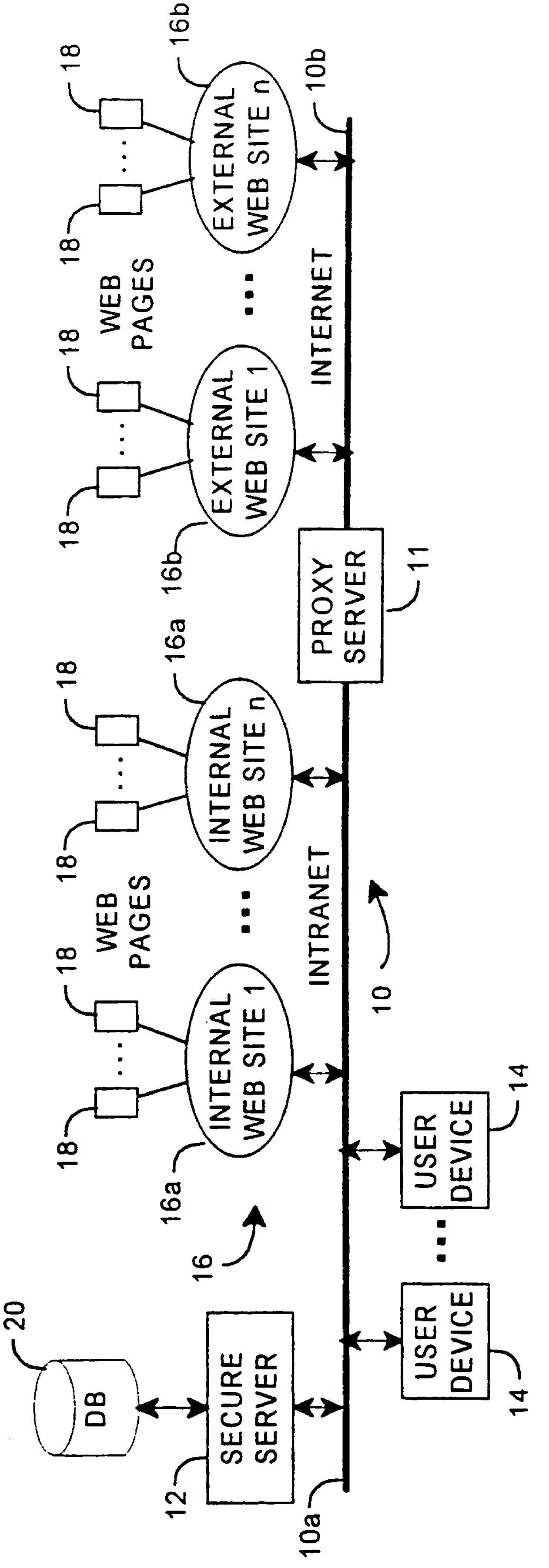
20
DB
SECURE SERVER
12
10a
16
16a
INTERNAL WEB SITE 1
18
18
18
WEB PAGES
INTERNAL WEB SITE n
18
18
16a
INTRANET
10
USER DEVICE
14
USER DEVICE
14
PROXY SERVER
11
16b
EXTERNAL WEB SITE 1
18
18
18
WEB PAGES
INTERNET
EXTERNAL WEB SITE n
18
18
16b
10b

FIG. 1

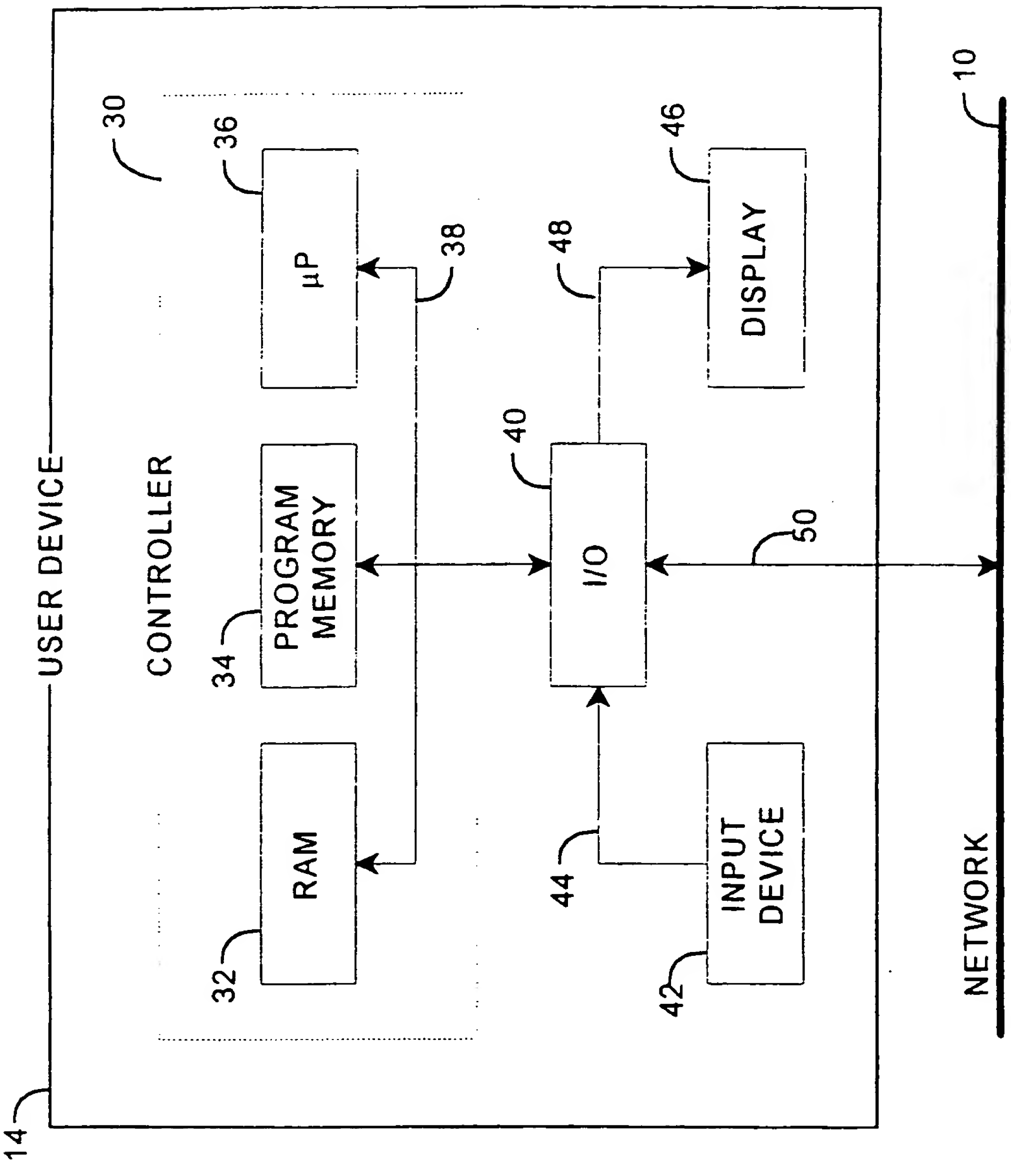
USER DEVICE
14
CONTROLLER
30
RAM
32
PROGRAM MEMORY
34
µP
36
38
I/O
40
INPUT DEVICE
42
44
DISPLAY
46
48
50
NETWORK
10

FIG. 2

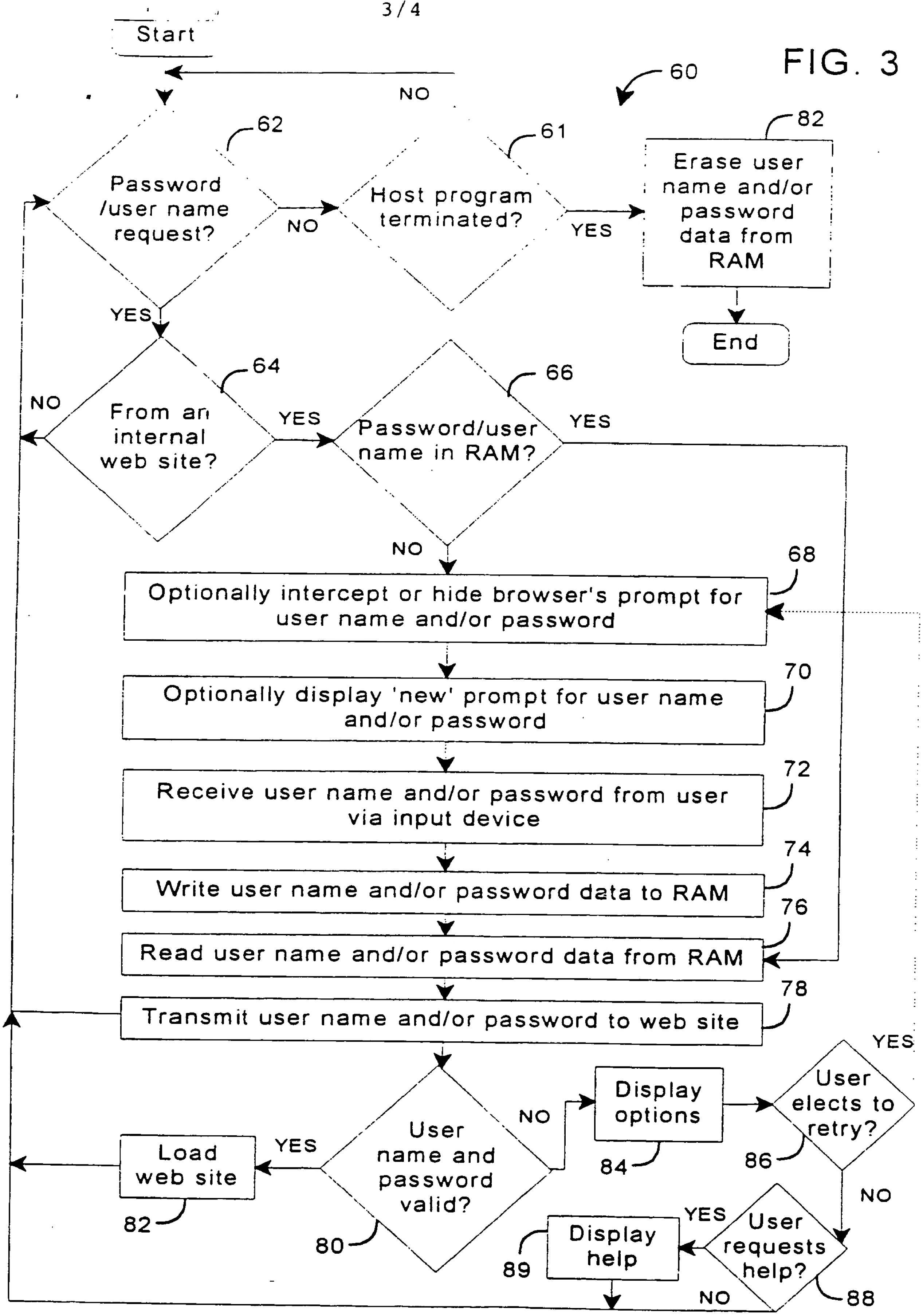

FIG. 3

Start
60
NO
62
Password /user name request?
NO
61
Host program terminated?
YES
82
Erase user name and/or password data from RAM
End
YES
NO
64
From an internal web site?
YES
66
Password/user name in RAM?
YES
NO
68
Optionally intercept or hide browser's prompt for user name and/or password
70
Optionally display 'new' prompt for user name and/or password
72
Receive user name and/or password from user via input device
74
Write user name and/or password data to RAM
76
Read user name and/or password data from RAM
78
Transmit user name and/or password to web site
YES
Load web site
82
User name and password valid?
80
NO
Display options
84
User elects to retry?
86
YES
NO
User requests help?
88
YES
Display help
89
NO

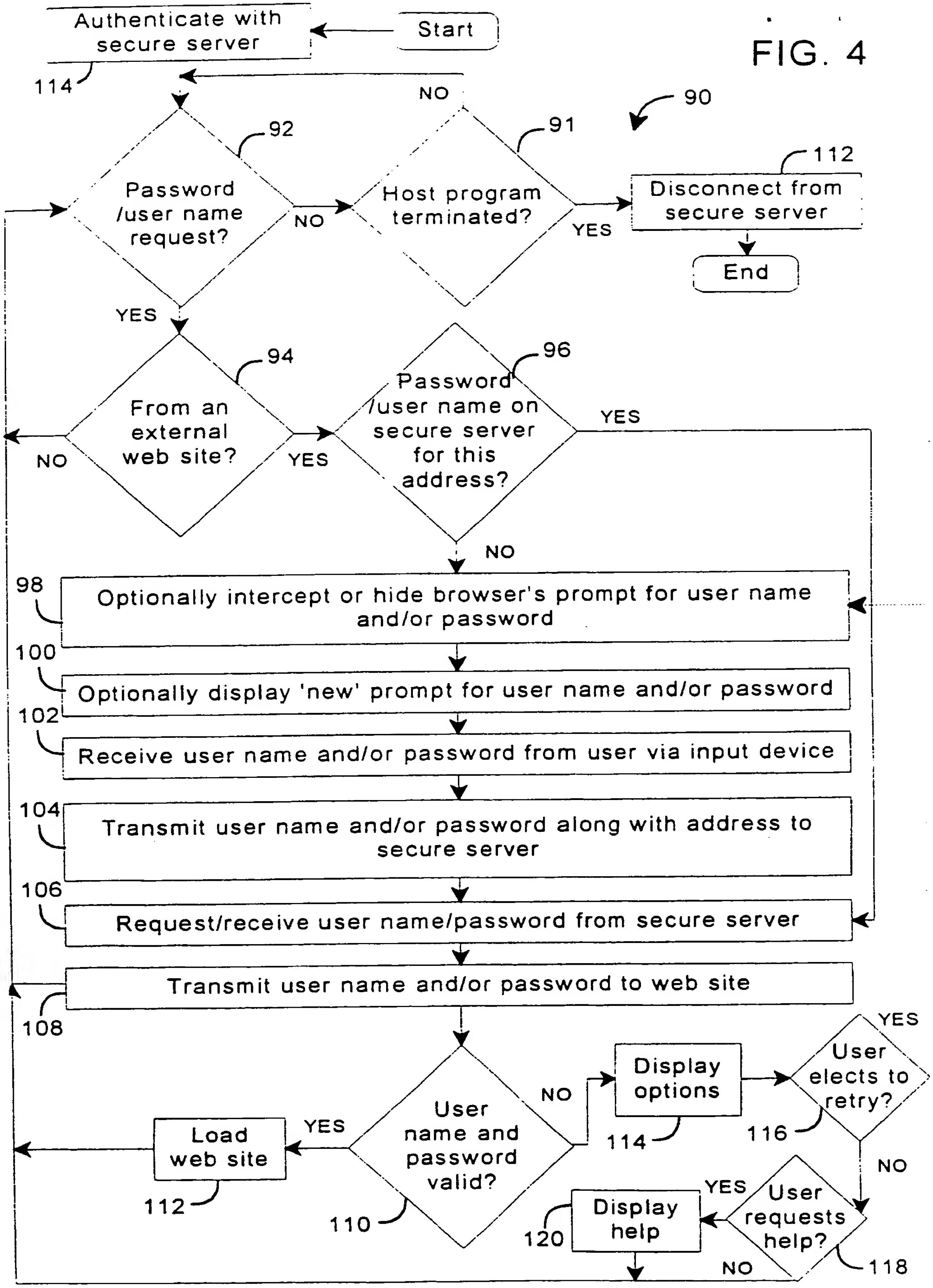
Start
Authenticate with secure server
114
90
Password /user name request?
92
NO
Host program terminated?
91
NO
YES
Disconnect from secure server
112
End
YES
From an external web site?
94
NO
YES
Password /user name on secure server for this address?
96
YES
NO
98
Optionally intercept or hide browser's prompt for user name and/or password
100
Optionally display 'new' prompt for user name and/or password
102
Receive user name and/or password from user via input device
104
Transmit user name and/or password along with address to secure server
106
Request/receive user name/password from secure server
Transmit user name and/or password to web site
108
User name and password valid?
110
YES
Load web site
112
NO
Display options
114
User elects to retry?
116
YES
NO
User requests help?
118
YES
Display help
120
NO

FIG. 4